REMARKS

Independent claims 1 and 29

Claims 1-8 and 29-33 were rejected under 35 U.S.C. §103(a) as being unpatentable over Brown et al. et al. in view of Hwangbo and further in view of Sudia et al. Reconsideration and withdrawal of these rejections are respectfully requested.

Claim 1 recites:

> **the authority of the user defined within the second code portion of the certificate being verifiable by the server computer independently of the digital certificate by accessing, over the network, a store of authority information that is independent of the digital certificate and by matching the authority of the user defined within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information.**

Claim 29 recites:

> **code for accessing, over the network, a store of authority information that is independent of the digital certificate and that stores corresponding authority information, the accessing code being configured to match the authority of the user defined within the second code portion of the certificate to the corresponding authority information accessed from the independent store to validate the rights of the user to data and programs within the computing environment.**

Therefore, each claim recites that the authority of the user defined in the second code portion of the certificate is verifiable independent of the digital certificate. This is done, according to the claims, by accessing a store of authority information that is independent of the digital certificate and matching the authority information accessed from the independent store with the authority information defined within the digital certificate. If they match, the authority defined in the second portion of the digital certificate is verified (claim 1) or the rights of the user to data and programs within the computing environment defined within the second portion of the digital certificate are validated (claim 29).

It is respectfully submitted that both claims recite that the authority defined within the certificate is verifiable (or may be validated) by accessing a store of information that is independent of the digital certificate. Moreover, it is acknowledged that the primary combination to Brown et al. and Hwangbo do not teach or suggest such subject matter, which necessitated the addition of Sudia et al. to the applied combination.

The Office points to paragraphs [0132], [0171], and [0252] for a teaching of verifying the authority of the user defined within the second code portion of the certificate by the server computer independently of the digital certificate by accessing, over the network, a store of authority information that is independent of the digital certificate and by matching the authority of the user defined within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information, as claimed.

Sudia et al. rely upon a plurality of trusted devices (such as signing devices 1, 2, 3, 4 and 5 of Fig. 1), each associated with an authorizing agent (1a, 2a, 3a, 4a and 5a of Fig. 1), all coupled via a WAN/LAN 21. In Sudia et al., each of the trusted devices, as instructed by its associated authorizing agent(s), affixes a partial digital signature to a document (for example) to be digitally signed in response to the authorization of a quorum (predetermined number) of authorizing agents, as described in paragraph [0085]. Therefore, Sudia et al. teach that there is a plurality of trusted devices, and each trusted device is configured to affix only a partial signature, and only when requested to by a predetermined number of authorizing agents. Thereafter, the trusted device returns the fully signed result to the requester (if all other required trusted devices have already signed) or routes the partially signed result to the next trusted device in the protocol, as described in paragraph 4, lines 8-12:

than they can be processed. The message server presents messages to the signing device for signing, receives the signed (or partially signed) result, and either (a) returns the partially signed result to the requester, or (b) routes the result to the next device in the protocol. In order to receive and

The "authorizing agents" in Sudia et al. issue signing instructions to the trusted device to which he or she is associated. See paragraph [0054]. Each trusted device has a signature, as does each authorizing agent, and they are used for different purposes, as detailed in Sudia et al. at paragraph 55, lines 8-12:

erated for and certified as belonging to the specified user. In this manner, the system can continue to use the device's signature to verify the trust level of the device on any given transaction, while using the user's signature to attest to the user's identity and consent to the transaction. This allows the

The authority of an authorized agent, in Sudia et al., is the authority of the authorizing agent to request that his or her associated trusted device digitally sign the document or message – not to request that a server computer carry out a requested action. The list of such authorizing agents is maintained in an internal table (see Fig. 7),

as discussed in Sudia et al. at paragraph [0132] (one of the paragraphs referenced in the Official Action), of which lines 7-11 are reproduced below:

verification key for each authorizing agent. In the registration process, each signing device will also update an internally-stored table of particular authorizing agents who will be empowered to instruct the signing device to apply its partial signature. During routine operation, a signing device

Therefore, when requested to partially digitally sign a document or message, the trusted devices of Sudia et al. will consult their internal tables 26 to insure that the requestor is an authorizing agent and only thereafter will the trusted device partially sign the requested document or message.

In Claim 1, the digital certificate is issued to the user of the client computer. In contrast, Sudia et al. teaches a method of digitally signing a message or a document by processing a plurality of partial digital signatures by a plurality of trusted devices on behalf of a corresponding plurality of authorized agents. Therefore, Sudia et al. teach who may sign a document or message and how such document or message may be digitally signed (i.e., by sequential partial signing), whereas the claimed embodiment defines the structure of a digital certificate and the functionality associated therewith.

Specifically, the method detailed in Sudia et al. deals with authentication; that is, insuring that those signing a digital certificate (through the trusted devices) are who they purport to be and are authorized to request that their trusted device sign the document or message. Such information, in the claimed embodiment, would be placed in the first claimed portion:

> **wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field,**

and not in the claimed second portion that is configured to define an authority of the user to request that the server computer carry out a requested action, as claimed.

The internal tables (see, e.g., 23 in Fig. 7) of authorizing agents who are "empowered to instruct the signing device to apply its partial signature", according to Sudia et al., do not include any information as to the authorizing agent's authority, within the meaning of claim 1. Indeed, claim 1 recites that the authority in question is the:

authority of the user of the client computer to request that the server computer carry out the requested action

Sudia et al. do not teach or suggest any such authority defined within the internal tables of authorizing agents 23. Moreover, when the internal tables 23 of Sudia et al. are consulted, the certificate is not yet in existence (even partially), as the trusted device is still determining whether the requestor is listed as an authorizing agent so that it may partially sign the document or message.

Moreover, kindly note paragraph [0050] of Sudia et al., which states:

> [**0050**] **FIG. 2** shows a preferred architecture for a secure data center computer configuration **48**, where each signing device of **FIG. 1** preferably will be found. In addition to a signing device **29**, each data center configuration **48** additionally contains a separate message server **47**. The signing device **39** is dedicated to signing operations and is located in a physically secure location, such as a vault. There is no direct connection between the signing device and the external computer network. As will be discussed more fully below, the signing device **39** will be provided with a key share for multi-step signing **36**, its own device signature key **37**, table **38** identifying its authorizing agents, and a certificate for its public verification key **40**, a public key chosen to match its key share **36** (where the certificate is signed by the full KS_{SWA} via the multi-step method).

In contrast, claim 1 specifically requires that

> **the authority of the user defined within the second code portion of the certificate being verifiable by the server computer independently of the digital certificate by accessing, over the network, a store of authority information that is independent of the digital certificate**

That is, the authority defined in the second code portion of the certificate must be verifiable by the server computer independently of the digital certificate by accessing, over the network, a store of authority information that is independent of the digital certificate.

This claimed recitation is not taught or suggested by Sudia et al., which specifically state that the internal tables of authorizing agents are maintained as internal tables within the trusted

signing devices that have no direct connection to the external computer network, rendering the functionality claimed in claim 1 impossible for the architecture espoused by Sudia et al.

Therefore, Sudia et al., contrary to the claimed embodiment, do not teach certificates assigned a) to users, b) that define an authority of the certificate holder to request that the server carry out a requested action, - such as, for example,

> **access rights of the user to data and programs within the computing environment.**

as claimed in claim 7 - c) that is verifiable by accessing d) over the network of e) a store of authority information that is f) independent of the certificate. Sudia et al. also do not teach matching the authority information within the certificate to the corresponding authority information stored in the store of authority information, as claimed herein.

Therefore, mindful of the requirement to consider the references of an applied combination of references collectively, the Office notes that Brown fails to teach a certificate assigned to a user of a client computer having a first code portion and a second code portion and that Hwangbo is relied on for its teaching of a certificate having first and second code portions. It falls to the Sudia et al. reference, therefore, in combination with Brown and Hwangbo, to teach or to suggest the claimed subject matter. However, a person of ordinary skill in the art would not be motivated to devise the claimed embodiments. Instead, such a person of ordinary skill in the art in full possession of Brown-Hwangbo-Sudia would, instead, be motivated to apply the teachings of Brown and Hwangbo to those of Sudia et al., and would partially sign (as taught by Sudia et al.) a document or message with a digital certificate (as taught by Brown), and the digital certificate would include a first code portion and a second code portion as taught by Hwangbo. The identity of authorizing users, in such a combination, would be stored within internal tables of a trusted signing device, as taught by Sudia et al. Those internal tables,

moreover, would be consulted by the trusted signing device without accessing the network, as explicitly taught by Sudia et al., and without matching the authority information within the certificate to corresponding authority information stored in the store of information that is accessed over the network, as also claimed herein. Nothing in the applied combination, moreover, teaches or suggests the authority in question is the authority to request a server computer to carry out a requested action, as claimed herein. In Sudia et al., for example, the agents are "authorized" not to request that a server carry out a requested action, but to simply request that the trusted signing devices digitally sign the document or message in question.

As the claimed embodiments are wholly unsuggested by the applied combination of references, reconsideration and withdrawal of the 35 U.S.C .§103(a) rejections of claims 1 and 29 and their respective dependent claims are, therefore, respectfully requested.

Independent Claims 9 and 15

Claims 9-13 and 15-19 are rejected under 35 U.S.C. §103(a) as being unpatentable over Brown et al. in view of Sudia et al. Reconsideration and withdrawal of these rejections are respectfully requested.

Claim 9 recites:

> **validating the authority information included within the received certificate by accessing a store of authority information that is coupled to the network and that is independent of the received certificate and by matching the authority information included within the received certificate to authority information that is associated with the user and that is stored in the accessed independent store of authority information, and**

Claim 15 recites:

> **authorization validating code configured to enable validation of the authority information within the received certificate against corresponding authority information for the user stored in a data structure that is coupled to the network and that is independent of the received certificate by accessing the data structure over the network and by matching the authority information included in the received certificate to the corresponding authority information stored in the accessed data structure.**

As with claims 1 and 29, independent claims 9 and 15 require that the verification/validation of the authority information within the received certificate be carried out against corresponding authority information accessed from a store of authority information that is independent of the received certificate. As such, the above arguments are equally applicable here. Rather than repeating them nearly *verbatim*, they are simply incorporated herein by reference, as if repeated in full.

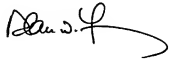
In short, the Brown et al.-Sudia et al. combination does not teach or suggest to verify the authority of the certificate holder (as opposed to the identity of the agent in the internal tables, as in Sudia et al.) by accessing a store of authority information, over the network, that is independent of the received certificate. Again, Sudia et al. do not remedy the acknowledged shortcomings of the Brown reference, because Sudia et al. do not teach certificates assigned a) to users of a client computer b) that define an authority of the certificate holder to request that the server carry out a requested action c) that is verifiable by accessing d) over the network of e) a store of authority information that is f) independent of the certificate. Sudia et al. also do not teach matching the authority information within the certificate to the corresponding authority information stored in the store of authority information, as claimed herein.

Therefore, the Brown-Sudia et al. combination fails to teach or to suggest the claimed embodiments of independent claims 9 and 15. Reconsideration and withdrawal of the rejections

of claims 9 and 15 and that of their respective dependent claims are, therefore, respectfully requested.

The Office is respectfully requested to reconsider the finality of the Office Action mailed May 24, 2007 and to allow this application. If any unresolved issues remain, please contact the undersigned attorney of record at the telephone number indicated below and whatever is necessary to resolve such issues will be done at once.

Respectfully submitted,



Date: August 24, 2007

By: _____

Alan W. Young
Attorney for Applicant
Registration No. 37,970

YOUNG LAW FIRM, P.C.
4370 Alpine Rd., Ste. 106
Portola Valley, CA 94028
Tel.: (650) 851-7210
Fax: (650) 851-7232

\\Ylfserver\ylf\CLIENTS\ORCL\5881 (OID-2003-142-01)\5881 AMEND.4.doc